

1 **CARNEY BATES & PULLIAM, PLLC**
2 Joseph Henry (“Hank”) Bates (CA #167688)
3 hbates@cbplaw.com
4 Randall K. Pulliam
5 rpulliam@cbplaw.com
6 11311 Arcade Drive, Suite 200
7 Little Rock, AR 72212
8 Telephone: (501) 312-8500
9 Facsimile: (501) 312-8505

10
11
12
13 Attorneys for Plaintiffs
14 Napoleon Ebarle and Jeanne Stamm
15
16
17
18
19
20
21
22
23
24
25
26
27
28

13 UNITED STATES DISTRICT COURT

14 NORTHERN DISTRICT OF CALIFORNIA

16 NAPOLEON EBARLE and JEANNE
17 STAMM, on behalf of themselves and all
18 others similarly situated,

19 Plaintiffs,
20 vs.

21 LIFELOCK, INC.,

22 Defendant.

19 Case No:

20 **CLASS ACTION COMPLAINT**

21 1. VIOLATIONS OF THE ARIZONA
22 CONSUMER FRAUD ACT (ARIZ.
23 REV. STAT. § 44-1522(A))
24 2. DECLARATORY JUDGMENT

1 COMES NOW, Plaintiffs Napoleon Ebarle and Jeanne Stamm (“Plaintiffs”), who bring this
2 Complaint against Defendant LifeLock, Inc. (“Defendant” or “LifeLock”), and allege as follows:

3 **INTRODUCTION**

4 1. This is a consumer class action arising out of LifeLock’s false, misleading and
5 fraudulent representations and material omissions regarding its ability to protect consumers from
6 identity theft.

7 2. LifeLock markets itself as the “leading provider of proactive identity theft protection
8 services for consumers and identity risk and credit worthiness assessment for enterprise.” Upon this
9 self-proclaimed title, LifeLock offers the following fee-based membership plans to consumers
10 (collectively referred to as the “Membership Plans”): LifeLock Standard, LifeLock Advantage, and
11 LifeLock Ultimate Plus (described more fully below). Each of LifeLock’s Membership Plans is
12 governed by LifeLock’s Service Terms and Conditions, which specifically provides that

13
14
15 The Service Terms and any Services provided hereunder will be governed by the laws
16 of the State of Arizona, without regard to any laws that would direct the choice of
17 another state’s laws and, where applicable, will be governed by the federal laws of the
United States.

18 3. LifeLock markets, offers, and sells its Membership Plans as providing (1) the “most
19 comprehensive identity theft protection in the industry,” and (2) service 24 hours a day, 7 days a
20 week, 365 days a year. LifeLock further represents or creates the impression that its present
21 technology is adequate to safeguard its customers’ personal information and maintain necessary
22 security standards. In addition, LifeLock represents or creates the impression that it is compliant
23 with the terms of a settlement LifeLock entered into with the Federal Trade Commission (“FTC”) in
24 2010 (referred to herein as the “FTC Settlement”).

25 4. Despite its representations, Defendant has (a) failed to adequately disclose that its

1 service is subject to frequent delays and/or freezes; (b) failed to implement and maintain technology
2 to deliver and maintain security standards as promised; (c) failed to maintain compliance with the
3 FTC Settlement; and (d) inadequately handled cancellation requests to the detriment of its
4 consumers.

5 5. As such, Defendant has engaged in deceptive marketing and sales practices in
6 connection with its Membership Plans in violation of the Arizona Consumer Fraud Act, Ariz. Rev.
7 Stat. § 44-1522 (A).

9 6. Upon information and belief, as a result of their unfair, deceptive, and unconscionable
10 practices, Defendant has amassed substantial sums of money from the monthly fees paid by
11 consumers, including Plaintiffs, for these Membership Plans.

12 **PARTIES**

14 7. Plaintiff Napoleon Ebarle is a resident of California and subscriber, during all
15 relevant times hereto, to LifeLock.

16 8. Plaintiff Jeanne Stamm is a resident of California and subscriber, during all relevant
17 times hereto, to LifeLock.

18 9. Defendant LifeLock is a Delaware corporation with its principal executive offices at
19 60 East Rio Salado Parkway, Suite 400, Tempe, Arizona 85281. LifeLock conducts business
20 throughout California and the United States. It is currently estimated that LifeLock provides identity
21 theft services to over 3 million subscribers.

23 **JURISDICTION AND VENUE**

24 10. This Court has subject matter jurisdiction over this action under the Class Action
25 Fairness Act of 2005, which, inter alia, amends 28 U.S.C. § 1332 to add subsection (d), which
26 confers jurisdiction over class actions where, as here, “any member of a class is a citizen of a State

1 different from any other Defendant,” and the aggregated amount in controversy exceeds five million
 2 dollars. *See* 28 U.S.C. § 1332(d)(2) and (6).

3 11. This Court has jurisdiction over Defendant because it does business in California and
 4 upon information and belief Defendant’s conduct that gives rise to this complaint, as further
 5 described below, occurred within and/or was implemented, authorized, or ratified in California.
 6

7 12. In accordance with 28 U.S.C. § 1391, venue is proper in this district because a
 8 substantial part of the conduct complained of herein occurred in this District.
 9

COMMON FACTUAL ALLEGATIONS

I. Background, Prior Litigation, and the FTC Settlement

11 13. LifeLock was founded in 2005 by Richard Todd Davis (“Davis”) and Robert J.
 12 Maynard, Jr. (“Maynard”).
 13

14 14. From the outset, LifeLock’s business model was premised on placing and renewing
 15 “fraud alerts” on its customers’ credit files. A “fraud alert” is a 90-day alert credit reporting
 16 agencies place on a consumer’s credit file when requested to do so by the consumer or an authorized
 17 representative. To request a “fraud alert,” a consumer must have a good faith belief that he or she or
 18 it is, or is about to be, the victim of a fraud or related crime, including identity theft. The “fraud
 19 alert” gives notice to creditors accessing the consumer’s credit report that the consumers do not
 20 authorize the establishment of new credit, the issuance of additional cards on existing accounts, or an
 21 increase in the credit limit on an existing account.
 22

23 15. In 2006, LifeLock began an aggressive advertising campaign wherein Davis, Chief
 24 Executive Officer (“CEO”) of LifeLock, put his social security number on the side of a truck and
 25 claimed LifeLock made his personal data useless to criminals.
 26

27 16. The following year, 2007, it was exposed that Davis had become the victim of
 28

1 identity theft. Upon information and belief, Davis has had his identity stolen no less than 13 times
2 since 2006, despite being a LifeLock subscriber. As such, Davis' claim that LifeLock made his
3 personal data useless to criminals was proven to be a falsehood.

4 17. Notwithstanding, upon information and belief, LifeLock continued to market and sell
5 its products using the same and/or substantially similar marketing ploys.

6 18. In 2008, Experian Information Solutions, Inc. ("Experian"), a credit reporting agency,
7 filed suit against LifeLock alleging that LifeLock's practice of placing and renewing "fraud alerts"
8 under consumers' names violated the federal Fair Credit Reporting Act ("FCRA") because the
9 statutory language excludes corporations such as LifeLock from placing "fraud alerts". According
10 to court documents, LifeLock called Experian's fraud hotline up to 15,000 times a day to request
11 "fraud alerts."

12 19. In an order granting partial Summary Judgment in favor of Experian, the Honorable
13 Andrew J. Guilford agreed with Experian, finding that under the language of the statute and its
14 legislative history, "the FCRA embodies an established public policy against companies like
15 LifeLock placing fraud alerts on behalf of consumers." *See Experian Information Solutions, Inc. v.*
16 *LifeLock Inc.* (Case No. SACV08-00165 AG), Order Granting Motion for Partial Summary
17 Judgment, attached hereto as Ex. 1. Accordingly, the very premise of LifeLock's promised
18 protections, *i.e.* the Company setting fraud alerts on behalf of its consumers, was declared unlawful.

19 20. That same year, the FTC filed suit against LifeLock alleging that the Company's
20 services did not prevent identity theft, as represented, and did not provide many of the protections
21 claimed by LifeLock. The FTC alleged that LifeLock made material misrepresentations and/or
22 omissions of material fact in violation of Section 5(a) of the FTC Act by representing and/or creating
23 the impression, among others, that (a) LifeLock stops identity theft before it happens, (b) LifeLock
24

1 offers a proven solution to identity theft, and (c) LifeLock guarantees identity-theft from ever
2 happening. Thirty-five State Attorney Generals (referred to as the “State AGs”) joined the FTC’s
3 action.

4 21. In resolution of the claims brought by the FTC, LifeLock and the FTC entered into a
5 Final Stipulated Judgment and Order for Permanent Injunction and Other Equitable Relief as to
6 Defendants LifeLock and Davis (the “FTC Order”), wherein LifeLock and Davis and “their officers,
7 agents, servants, and employees and all persons in active concert of participation with any of them . .
8 .” were “permanently restrained and enjoined” from the following:

9

10 A. in connection with the advertising, distributing, promoting, offering for
11 sale, or sale of any product, service, or program designed for the purpose
12 of preventing, mitigating, or recovering from any form of identity theft as
13 defined in 18 U.S.C. § 1028, misrepresenting in any manner, expressly or
14 by implication:

15

16 1. that such product, service, or program provides complete protection
17 against all forms of identity theft by making customers’ personal
18 information useless to identity thieves;

19 2. that such product, service, or program prevents unauthorized changes
20 to customers’ address information;

21 3. that such product, service, or program constantly monitors activity on
22 each of its customers’ consumer reports;

23 4. that such product, service, or program ensures that a customer will
24 always receive a phone call from a potential creditor before a new
25 credit account is opened in the customer’s name;

26 5. the means, methods, procedures, effects, effectiveness, coverage, or
27 scope of such product, service, or program;

28 6. the risk of identity theft to consumers;

7. whether a particular consumer has become or is likely to become a
victim of identity theft; and/or

8. the opinions, beliefs, findings, or experiences of an individual or group of consumers related in any way to any such product, service, or program.

Such products, services, or programs include, but are not limited to, the placement of fraud alerts on behalf of consumers, searching the internet for consumers' personal data, monitoring commercial transactions for consumers' personal data, identity theft protection for minors, and guarantees of any such product, services, or programs.

B. misrepresenting in any manner, expressly or by implication, the manner or extent to which they maintain and protect the privacy, confidentiality, or security of any personal information collected from or about consumers.

22. The FTC Order further ordered that LifeLock (as well as any business entity controlled by Davis that collects, maintains, or stores personal information from or about consumers) “establish and implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to the entity’s size and complexity, the nature and scope of the entity’s activities, and the sensitivity of the personal information collected from or about consumers”

23. In this same vein, the FTC order required LifeLock to make an initial assessment and biennial assessments for twenty years on the effectiveness of its safeguards.

24. The FTC Order also obligated LifeLock to pay \$11 million to the FTC, to be used for equitable relief to injured consumers, and \$1 million to the State AGs.

II. LifeLock's Relationship With Its Subscribers

25. As previously noted, LifeLock markets, offers, and sells the following fee-based Membership Plans: LifeLock Standard, LifeLock Advantage, and LifeLock Ultimate Plus.

26. LifeLock Standard offers identity theft detection and alerts within its network. Lost

1 wallet protection, address change verification, black market website surveillance and reduced pre-
 2 approved credit card offers for \$9.99/mo.

3 27. LifeLock Advantage offers LifeLock Standard services plus fictitious identity
 4 monitoring, court records scanning, data breach notifications, credit reports and scores, and financial
 5 account activity alerts for \$19.99/mo.

6 28. LifeLock Ultimate Plus protection provides LifeLock Advantage services plus bank
 7 account takeover alerts, enhanced credit application alerts, file-sharing network searches, sex
 8 offender registry reports, credit reports and scores, and monthly credit score tracking for \$29.99.

9 29. As an add-on service, a subscriber of one of these three Membership Plans can enroll
 10 in LifeLock Junior, which is marketed and sold as providing monitoring services for the member's
 11 children's personal information. LifeLock Junior protection purportedly provides identity theft
 12 detection and alert notifications, credit file detection, black market website surveillance, file-sharing
 13 network searches, and a \$1 million total service guarantee. According to LifeLock, "LifeLock
 14 Junior – it's relentless protection for your kids and peace of mind for you."

15 30. Each of LifeLock's Membership Plans is governed by LifeLock's Service Terms and
 16 Conditions, which specifically provide that

17 These LifeLock Service Terms and Conditions (the "Service Terms") are a legally binding
 18 agreement between LifeLock, Inc. ("LifeLock," "we" "our" or "us") and you ("you," "your"
 19 or "yours"), and describe the terms under which you agree to use the LifeLock identity
 20 programs, including any applicable Stolen Identity Insurance (the "Protection Programs"),
 21 credit monitoring service (the "Credit Monitoring Service") and any other service or product
 22 which may be made available to you by us for which you have registered or enrolled or have
 23 been registered or enrolled by an authorized third party (collectively the "Services" and
 24 individually a "Service").

25 31. In addition, the Service Terms and Conditions provide as follows:

26 The Service Terms and any Services provided hereunder will be governed by the laws
 27 of the State of Arizona, without regard to any laws that would direct the choice of
 28 another state's laws and, where applicable, will be governed by the federal laws of the

1 United States.

III. Defendant's Products Are Marketed, Offered, and Sold to Consumers in an Unfair, Misleading, and Deceptive Manner.

32. LifeLock advertises heavily on the television, internet, and radio. It claims, via its website, to provide “comprehensive identity theft protection” that “helps safeguard your finances, credit and good name,” and promises to guarantee its services up to \$1,000,000.

33. More particularly, LifeLock markets, offers, and sells each of its Membership Plans as providing the following: (a) protection from fraud or unauthorized account charges; (b) a solution to financial security; (c) live member support 24/7/365 and up-to-the-minute “alerts” of any threat of identity theft; and (d) a \$1 million total service guarantee.

34. LifeLock advertises and sells its Membership Plans on the representation that "LifeLock's patented alert technology gives you the opportunity to confirm your identity before a new account such as a retail card, auto loan or new wireless phone is opened with your information."

35. LifeLock further represents that it will keep its customers timely informed through use of its “Identity Alert System”. According to its website, LifeLock promises the following:

Alerts When You Need Them

With our patented LifeLock Identity Alert system, as soon as we detect a threat to your identity, you'll be notified by text, phone, or email, to help stop thieves before they do damage. So while you're out there connecting to the world, we'll be here helping to keep your personal information safe.

36. Defendant represents that it provides continuous “alert” services, maintaining that its team works 24 hours a-day, 7 days a week, 365 days a year. Specifically, Defendant touts:

Need Help? We're Here all the Time.

Our award-winning Member Services agents are on the job every minute of every day, including holidays. Call or contact us online whenever you need help or have questions. If you do become a victim, our Certified Resolution Specialists know exactly what to [do]. That's why millions trust LifeLock with their identity theft

1 protection.

2 **A. A LifeLock Insider Reveals that LifeLock Misrepresents the Scope and**
Effectiveness of Its Alert Services.

3 37. In a complaint filed on July 8, 2013 for wrongful termination (*see Burke v. LifeLock,*
 4 *Inc.*, No. 13-CV-1355 (D. Ariz.)), Stephen P. Burke (“Burke”), a Senior Financial Analyst with
 5 LifeLock from February 1, 2010 to March 2013, revealed that during the period of his employment,
 6 LifeLock

7 had and continues to have widespread system problems in processing [] alerts and
 8 sending them out to the customers as promised in its national marketing campaigns.
 9 The problem of timely informing customers that their credit information was accessed
 10 is so widespread that Defendant instituted a code freeze. In essence, Defendant is
 11 deliberately ‘stepping on the brakes’ with regard to sending this critical information
 12 to customers on a timely basis, and worse, often choosing not to send these alerts out
 13 at all. This practice has been referred to as “throttling.”

14 *See Ex. 2: Burke Compl., ¶ 13.*

15 38. Burke alleged that he “first learned of an issue with LifeLock’s alert notification
 16 services to customers through an e-mail chain forwarded to him in late November 2012 by John
 17 Lenstohm (“Lenstohm”), [LifeLock’s] Director, Direct Response.” *Id.* at ¶ 15.

18 39. Burke further recounted that he reported the problems of delayed alerts, diminished
 19 alert notification service, and “throttling” of alerts with the following LifeLock officers and
 20 employees, among others: Lenstohm, Director, Direct Response; Erick Dickens, Vice President of
 21 Marketing; Amanda Mellon, Senior Manager; Brent Hazel, Manager; Melinda Keels, Finance; and
 22 Gregory Lim, Burke’s immediate supervisor.

23 40. Burke further averred that he raised concerns to the officers and employees identified
 24 in the preceding paragraph about the effects of not sending out alerts, specifically addressing that
 25 “throttling” might violate the FTC Order. Burke also recommended that LifeLock “adjust its
 26 marketing messaging to reflect this diminished service.” *Id.* at ¶¶ 16, 19.

1 41. In February 2014, LifeLock settled Burke's wrongful termination suit for an
 2 undisclosed amount.

3 **B. A Second LifeLock Insider Confirms Delays and Shut-Downs of LifeLock's**
 4 **Alert Notification Services and Further Reveals that LifeLock's Technology Is**
Inadequate to Provide the Protections Promised.

5 42. On the heels of the Burke settlement, Michael D. Peters ("Peters"), LifeLock's Chief
 6 Information Security Officer from approximately May 24, 2013 through July 29, 2013, filed a
 7 complaint against LifeLock for wrongful termination and violation of whistleblower protection laws,
 8 a suit that remains ongoing.

9 43. In his complaint against LifeLock, Peters alleges that upon commencing work at
 10 LifeLock, he immediately began an initial risk assessment of the Company. Peters states that prior
 11 to his risk assessment, the Company had never conducted a bona fide risk assessment. Ex. 3: Peters
 12 Compl. ¶ 17.

13 44. Peters recounts that the findings of his assessment included discovery of multiple
 14 examples of LifeLock engaging in misleading, unfair, and/or deceptive practices, including, among
 15 others, the following:

- 16 • LifeLock's manager of database administration, Jacqueline Hufford-Jensen, signed a
 17 Sarbanes-Oxley audit verifying that the information contained in that audit was true
 18 and correct even though the time period she was attesting to predated her hiring date
 19 at LifeLock.
- 20 • LifeLock's director of internal audits, Tony Valentine, had collected evidence from
 21 the information security team that existed prior to Peters's arrival related to access
 22 logging, audit logging, audit log reviews, network security controls, and data
 23 leakage controls that either (1) did not truly exist because the technology was still in
 24

1 boxes; or (2) LifeLock lacked the staff to keep track of everything; or (3) such
2 reviews were not actually conducted.

3 • LifeLock employee Dave Bridgman reported that LifeLock's current practice was to
4 manipulate the customer alerts sent to its elderly customers. LifeLock would turn
5 off or reduce the services alerting elderly customers to reduce the call volume
6 received by LifeLock's customer support center.

7 • LifeLock was in the process of finalizing a new product offering called PassLock.
8 This system was designed to allow customers to include their passwords for up to
9 ten accounts. PassLock would then crawl through hundreds of internet sites to
10 check the username and password supplied by the customer and report back to the
11 customer. The problem was that the database was not being protected with industry-
12 grade encryption. The database was predicted to contain millions of customer
13 credentials that would be devastating to consumers if a breach occurred. Moreover,
14 the system was going to utilize third-party cloud hosting business without that third
15 party's knowledge or consent. Technically, the PassLock crawling would be
16 identified by most service providers as intrusive, illegal, illegitimate, and then
17 blacklist the source address.

18 *Id.*

19 45. Peters further alleges that the risk assessment uncovered that LifeLock's technology
20 and security were ineffective to deliver the protections LifeLock promised. Specifically, Peters
21 determined that

22 • "LifeLock's internal capacity for governance implemented (policies, audit plan,
23 change controls, architecture review, etc.) was at 47% of the minimum to protect

1 LifeLock's customers and their sensitive information." (*Id.* at ¶ 18);

2

- 3 "LifeLock's technological security readiness (intrusion prevention, data leakage, data
- 4 encryption, access controls, physical security, etc.) was only at 27% of the minimum
- 5 to protect LifeLock's customers and their sensitive information." (*Id.* at ¶ 19); and
- 6
- 7 • "LifeLock's security vigilance (vulnerability testing, auditing, monitoring, awareness
- 8 education, event logging, incident management, etc.) was at 0% of the minimum to
- 9 protect LifeLock's customers and their sensitive information." (*Id.* at ¶ 20).

10 46. According to Peters, these deficiencies were due, in large part, to deficient staffing.

11 LifeLock only had two people responsible for security. One individual lacked technical skill and

12 only had minimal security experience. While the other had technical skills, he was newly out of

13 college and lacked experience. Peters determined that millions of consumers were at risk, which led

14 Peters to advise LifeLock Chief Financial Officer, Chris Power, and LifeLock Chief Information

15 Officer, Rich Stebbins, that LifeLock should immediately hire 12 information security professionals.

16 Peters reports that in response, LifeLock fired Peters, resulting in Peters filing suit. (*Id.* at ¶¶ 20-25.)

17 **C. LifeLock Fails to Inform Customers that It Cannot Lawfully Place "Fraud**

18 **Alerts" With Credit Reporting Agencies**

19 47. Despite the court's ruling in *Experian* (see ¶¶ 20-21 above), LifeLock's business

20 model and services have remained substantially unchanged since 2005. See

21 <http://consumerproductadvisor.com/lifelock-review/>. Indeed, on the website

22 www.lifelockblog.com/why-lifelock/, which has a 2015 copyright and was last visited by Plaintiffs'

23 counsel on January 14, 2015, LifeLock continues to represent that "LifeLock will request on your

24 behalf that fraud alerts be placed on your accounts – By doing these, creditors will use extra care to

25 identify who you are to investigate the validity of any transaction."

1 48. On this same website, LifeLock further represents that “If a child has a credit report,
 2 LifeLock will request that fraud alerts be placed on the child’s accounts.” *See*
 3 www.lifelockblog.com/why-lifelock/.

4 49. However, at no time does LifeLock inform consumers that under the statutory
 5 language of the FCRA, only an individual is allowed to place a “fraud alert,” either for themselves, or
 6 acting on behalf of or as a personal representative to another individual.
 7

8 50. Likewise, LifeLock fails to inform consumers that a federal court has previously
 9 ruled that placement of fraud alerts by LifeLock with any credit reporting agency violates public
 10 policy.

11 **D. LifeLock Fails to Disclose the True Nature of Its Service, and Then Inadequately**
 12 **and/or Unfairly Handles Cancellation Requests**

13 51. The Consumer Product Advisor reports that LifeLock’s products and services are
 14 marketed in a confusing and convoluted way, masking their limitations, exclusions, and restrictions,
 15 and making it impossible for consumers to knowingly determine what these products cover and
 16 whether they provide a worthwhile benefit.

17 52. For example, LifeLock’s marketing proclaims that membership in one of LifeLock’s
 18 Membership Plans provides “peace of mind.” However, Defendant’s “peace of mind” tagline
 19 misrepresents the true nature of the Membership Plans; specifically, that a majority of the services
 20 provided are available for free; that Defendant’s services have many hidden, variable, and narrow
 21 restrictions; that Defendant’s alert notification services are substantially diminished because of the
 22 Company’s practice of “throttling” alerts; and that Defendant’s monitoring services were not
 23 equipped to handle and protect a customer’s personal information as represented by LifeLock.
 24

1 53. In addition, upon information and belief, LifeLock fails to adequately inform its
 2 members that the Company only runs a credit report once a year and that the Sex Offender list
 3 maintained by LifeLock is not updated on a daily or weekly basis.

4 54. Upon further information and belief, Defendant's customer service representatives
 5 employ an array of deceptive tactics to thwart members' ability to cancel their Membership Plans.

6 55. According to various customer complaints posted on
 7 www.consumeraffairs.com/privacy/lifelock.html, LifeLock does not timely respond to cancellation
 8 requests and/or uses scare tactics to bully or mislead customers into believing that they are unsafe
 9 without LifeLock. Moreover, customers report that even after canceling their accounts, or at least a
 10 portion thereof, they continued to be billed by LifeLock for the canceled services.

12 **IV. Defendant's Policies, Procedures, and Practices Are in Violation of the FTC Order.**

13 56. As set forth above in ¶¶ 23 through 26, the FTC Order enjoins LifeLock from
 14 misrepresenting, expressly or by implication, "the means, methods, procedures, effects,
 15 effectiveness, coverage, or scope" of LifeLock's services.

17 57. Notwithstanding, throughout the Class Period, Defendant has made, and continues to
 18 make, material misrepresentations and omissions. For example, LifeLock has failed on an ongoing
 19 basis to disclose that its consumer alert notification services were subject to regular delays and were
 20 actively disabled by the Company. Thus, Defendant's representations that LifeLock offers
 21 "24x7x365" service support and up-to-the-minute "alerts" are misleading, at best.

23 58. Moreover, LifeLock has represented, on a continuous basis, and/or actively created
 24 the impression, and continues to create the impression, that its technology and safety protocols were
 25 and are sufficient to adequately protect its members private and confidential information as promised.
 26 However, as previously described herein, LifeLock's technology and personnel were deficient and

1 incapable of protecting the security, confidentiality, and integrity of personal information collected
 2 from or about consumers as promised.

3 **V. The FTC's Renewed Investigation of LifeLock**

4 59. Around the same time Peters filed his wrongful termination suit against LifeLock in
 5 federal court, Peters filed a whistleblower complaint with the FTC. As a result, in or about August
 6 2013, the FTC opened an investigation into LifeLock's current policies, procedures, and practices.
 7 Upon information and belief, the FTC investigation remains ongoing.

8 **FACTUAL ALLEGATIONS SPECIFIC TO NAMED PLAINTIFFS**

9 60. Plaintiff Napoleon Ebarle has been a member of LifeLock since at least 2012. In
 10 addition, Plaintiff Ebarle enrolled his wife and two minor children. Since his enrollment and based
 11 on LifeLock's representations and promises, Plaintiff Ebarle has paid LifeLock a fee of
 12 approximately \$40 a month for LifeLock's services.

13 61. Based on LifeLock's advertisements and representations, Plaintiff Ebarle understood
 14 and/or had the impression that LifeLock would protect against any attempt to steal his identity or
 15 fraudulently procure credit under his name, would contact him in the event of suspicious activity,
 16 and send him "up-to-the-minute" alerts. In accord with Plaintiff Ebarle's understanding, he
 17 submitted his, his wife's, and his children's personal information to LifeLock.

18 62. However, during his subscription, Plaintiff Ebarle experienced an incident with
 19 suspicious activity to his family's personal information. However, Plaintiff Ebarle did not receive
 20 the services and/or support promised by LifeLock.

21 63. Additionally, upon contacting LifeLock, Plaintiff Ebarle learned that despite paying
 22 for services for himself, his wife, and two children, LifeLock was not servicing the accounts for his
 23 wife and two children.

64. Plaintiff Jeanne Stamm subscribed to LifeLock in 2008. Since that time, Plaintiff Stamm has paid LifeLock a fee of approximately \$100 a year, or \$9 per month.

65. Based on LifeLock's advertisements and representations, Plaintiff Stamm understood and/or had the impression that LifeLock would protect against any attempt to steal her identity or fraudulently procure credit under her name and send her timely alert notification. Based on her understanding, Plaintiff Stamm submitted her personal information to LifeLock.

66. At no time relevant hereto was Plaintiff Stamm aware that LifeLock was not permitted to submit fraud alerts on her behalf; that LifeLock's consumer alert notification services were subject to regular delays and were actively disabled by the Company; or that LifeLock's technology and personnel were deficient and incapable of protecting the security, confidentiality, and integrity of personal information collected from or about consumers as promised.

67. As such, Plaintiffs were charged and paid fees for services that were not as represented, were illegal for the Company to perform, were non-existent, and/or virtually worthless.

CLASS ACTION ALLEGATIONS

68. Plaintiffs bring this action against LifeLock as a class action pursuant to the Federal Rules of Civil Procedure 23(a) and 23(b)(2) and (b)(3).

69. Plaintiffs seek certification of this action on behalf of the following class (the “Class”): all persons in the United States who are or were, during January 19, 2014 through the resolution of this matter (the “Class Period”) subscribers of LifeLock’s fee-based theft protection services. Excluded from the Class are Defendant, any parent, subsidiary, affiliate, or controlled person of Defendant, as well as the officers, directors, agents, servants or employees of Defendant and the immediate family members of any such person. Also excluded is any judge who may preside over this cause of action.

70. The exact number of the Class, as herein identified and described, is not known, but it is estimated to number in the thousands. The Class is so numerous that joinder of individual members herein is impracticable.

71. There are common questions of law and fact in the action that relate to and affect the rights of each member of the Class and the relief sought is common to the entire Class. In particular, the common questions of fact and law include:

- (A) Whether Defendant's alert notification services were subject to regular delays and/or shut-downs;
- (B) Whether Defendant failed to maintain compliance with the FTC Order;
- (C) Whether Defendant's technology and safeguards were deficient to deliver the protections as promised;
- (D) Whether Arizona law applies to the putative Class; and
- (E) Whether members of the Class have sustained damages, and, if so, in what amount.

72. The claims of the Plaintiffs, who are representative of the Class herein, are typical of the claims of the proposed Class, in that the claims of all members of the proposed Class, including the Plaintiffs, depend on a showing of the acts of Defendant giving rise to the right of Plaintiffs to the relief sought herein. There is no conflict between the individually named Plaintiffs and other members of the proposed Class with respect to this action, or with respect to the claims for relief set forth herein.

73. The named Plaintiffs are the representative parties for the Class, and are able to, and will fairly and adequately protect the interests of the Class. The attorneys for Plaintiffs and the Class are experienced and capable in complex civil litigation, consumer fraud litigation and class actions.

74. The class action procedure is superior to all other available methods for the fair and efficient adjudication of this controversy. This action would permit a large number of injured persons to prosecute their common claims in a single forum simultaneously, efficiently, and without unnecessary duplication of evidence and effort. Class treatment also would permit the adjudication of claims by class members whose claims are too small and complex to individually litigate against a large corporate defendant.

COUNT I

75. Plaintiffs repeat and reallege all preceding paragraphs contained herein.

76. LifeLock's advertising and marketing made use of material misrepresentations and omissions, false promises, and deception in connection with the sale and advertisement of its services in violation of the Arizona Consumer Fraud Act, Ariz. Rev. Stat. § 44-1522(A).

77. Specifically, LifeLock used false, deceptive and misleading statements, and omitted material facts, concerning the scope and effectiveness of its services; LifeLock's ability to place fraud alerts under the FCRA; and the limitations, exclusions, and restrictions on LifeLock's services. For example, LifeLock omits from its advertising the fact that its consumer alerts are subject to regular delays and are actively disabled. In addition, LifeLock also fails to disclose the effects of not sending out alerts.

78. Likewise, LifeLock's advertisements and website were misleading, false, and/or deceptive regarding the efficacy of LifeLock's technology and safeguards.

79. LifeLock's advertisements, marketing, and customer service representatives purposely used inconsistent and confusing terms and/or high pressure sales tactics so as to confuse customers and prevent them from bringing legitimate claims and/or canceling their services.

80. Upon information and belief, LifeLock knowingly violated the terms of the FTC

Order and used false, misleading, and deceptive representations and/or omissions in the advertising, marketing, and sales of its services.

81. As a result of LifeLock's misrepresentations and omissions, LifeLock's members paid substantial fees, were injured and sustained damages in an amount to be proven at trial. These damages include, at a minimum, payments of monthly charges for services that were not as represented and payments for a service that is illegal for a company such as LifeLock to perform.

COUNT II
DECLARATORY JUDGMENT

82. Plaintiffs hereby repeat and reallege all preceding paragraphs contained herein.

83. An actual case and controversy within the meaning of the Federal Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202, which may be adjudicated by this Court exists between Plaintiffs and proposed class members, and the Defendant.

84. Plaintiffs and all members of the proposed class have, had, or were subscribers of one of Defendant's fee-based Membership Plans. Defendant's Terms and Conditions provide that its insureds are treated consistent with the requirements of the laws and regulations of Arizona. Thus, per the governing contract, Arizona law controls how the Defendant's customers must be treated by Defendant.

85. At the same time, the relationship between Defendant and its customers was subject to the FTC Order entered between Defendant and the FTC in 2010, which specifically enjoins LifeLock from misrepresenting, expressly or by implication, “the means, methods, procedures, effects, effectiveness, coverage, or scope” of LifeLock’s services.

86. Defendant, as a general policy and business practice, represented or created the impression that LifeLock's Membership Plans provide: (a) protection from fraud or unauthorized account charges or "peace of mind"; (b) a solution to financial security; (c) live member support

24/7/365 and up-to-the-minute “alerts” of any threat of identity theft; and (d) a \$1 million total service guarantee.

87. Accordingly, Defendant has violated, and continues to violate, Arizona law and the FTC Order and Plaintiffs are entitled to declaratory relief.

RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully request that this Court:

- a) determine that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class representatives, and approve Plaintiffs' Counsel as counsel for the Class;
- b) enter an order demanding that Defendant pay monetary damages to the Plaintiffs, and all proposed Class members;
- c) enter an order declaring that Defendant's actions are unlawful; and
- d) grant such other legal and equitable relief as the Court may deem appropriate, including costs and attorneys' fees.

V. JURY DEMAND.

Plaintiffs and the Class members hereby request a trial by jury.

Dated: January 19, 2015

Respectfully submitted,

By: /s/ Joseph H. Bates
CARNEY BATES & PULLIAM, PLLC
Joseph Henry ("Hank") Bates (CA #167688)
Randall K. Pulliam
11311 Arcade Drive, Suite 200
Little Rock, AR 72212
Telephone: (501) 312-8500
Fax: (501) 312-8505

Attorneys for Plaintiffs